Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 10, číslo 4/2008 **15. duben 2008**

4/2008

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1228 registrovaných odběratelů)

Obsah :

Příloha: ---

A. Hakin9 - jak se bránit ?

Věnováno paní Sylwia Hacieja a Martyna Zaczek

Vážení čtenáři,
pravděpodobně jste zaregistrovali, že po časopisu „***LINUX+“*** skončil na našem trhu i časopis „***Hakin9 - Jak se bránit?“*** .

Po Linux+ končí i Hackin9?
http://www.suseportal.cz/kategorie/novinka/po-linux-konci-i-hackin9

Linux+ a Hackin9 končí na českém trhu
http://www.maxiorel.cz/linux-hackin9-konci-na-ceskem-trhu

Český linuxový tisk? Nemáme.
http://svatas.blog.root.cz/0803/cesky-linuxovy-tisk-nemame

http://www.abclinuxu.cz/zpravicky/hackin9-nasleduje-osud-linuxplus-v-cr-konci
www.abclinuxu.cz/zpravicky/hackin9-nasleduje-osud-linuxplus-v-cr-konci

Úvodník našeho e-zinu není věnován hodnocení, přínosu, kvalitě, zájmu čtenářů nebo vysoké prodejní ceně těchto časopisů. Je pouze informací o praktikách redakce a upozorněním pro ty, kteří budou v budoucnu zvažovat případnou spolupráci a to zejména s redaktory Sylwia Hacieja a Martyna Zaczek, protože předpokládám, že v integrované Evropě se s nimi opět budete moci setkat.

Není to tak dávno, kdy zde redakce začínala a zoufale hledala české autory. Nyní mne mrzí, že jsem jim dal kontakty a tipy na některé své bývalé kolegy a žáky. Nemohl jsem tušit, že za články, které redakci předají k otištění, nedostanou zaplaceno. Touto cestou se jim proto všem omlouvám.

Ano, redakce totiž za články, které přijala a otiskla, přestala autorům přibližně od léta 2007 platit. Zjistil jsem to, když jsem si u kolegů náhodně ověřoval, zda nezaplacení mého honoráře byla jen náhoda nebo se jim to stalo také. Z jejich odpovědí jsem zjistil, že redakce ve svém platebním režimu nevynechala jen mne, ale prakticky všechny autory na které jsem se s tímto dotazem obrátil.

Scénář komunikace redakce s autory se opakoval následovně, po včasném odevzdání článku se autor začal pídit po honoráři. Po několika urgencích byla vystavena autorská smlouva (nejdříve byl autor nesmyslně požádán, aby redakci na článek vystavil fakturu!). Splatnost smlouvy byla uvedena jeden měsíc po podpisu. Když si autor po několika týdnech vzpomněl, že vlastně nic neobdržel, byl ujištěn, že v nejbližším výplatním termínu se tak stane. Nestalo. Na další dotaz/urgenci bylo autoru oznámeno, že redakce prověří, proč se tak dosud nestalo. Nic se nedělo a na další, byť opakované urgence redakce přestala odpovídat. Následně zaslané e-maily zástupci redakce četli (přišla notifikace), ale neměli již ani tu úctu k autorům, aby jim odpověděli, omluvili se, vysvětlil, proč nemohou zaplatit….

Teprve z e-mailové korespondence se ukázalo, že každý z těch autorů, které jsem oslovil, se domníval, že problém má jen on sám a naivně očekával, že se vše vyřeší...

Jenže nic se nedělo a pak přišel první duben - Apríl. Autoři v tento den konečně obdrželi z redakce e-mail. Místo očekávaného vysvětlení, zde bylo poděkování za úspěšnou spolupráci a oznámení o ukončení činnosti. Ani slovo o tom, jak a zde bude dluh řešen, ani slovo vysvětlení ani slovo omluvy….
E-mail přikládám v úplném a doslovném znění.

---------- Původní zpráva ----------
Předmět: Fw: Magazín hakin9- jak se bránit?
Od: "Sylwia Hacieja" <sylwia.hacieja@software.com.pl>
Datum: 1 Duben 2008, 10:39
Komu: "Sylwia Hacieja" <sylwia.hacieja@software.com.pl>

Dobrý den,
chtěla bych Vám poděkovat za sebe a za celou naši redakci hakin9- jak se bránit? za skvělou spolupráci.
Z organizačních důvodů bohužel s vydaváním magazínu hakin9 na českem trhu končíme. Poslední číslo, kreré bude uvedeno do prodeje je 3/2008.
Děkují Vám ještě jednou a přejí mnoho úspěchů nejen v profesním životě.
V případě dotazů pište, prosím na adresu: cz@lpmagazine.org
S pozdravem
Sylwia Hacieja
Junior Product Manager
Hakin9 CS
http://www.hakin9.org/cz/haking.html
tel. +420 24 601 91 31
Software - Wydawnictwo Sp. z o.o
ul. Bokserska 1, 02-682 Warsaw, Poland
Sąd Rejestrowy: Sąd Rejonowy dla m.st. Warszawy,
XIII Wydział Krajowego Rejestru Sądowego
KRS: 0000053777
NIP: PL9511821441
kapitał zakładowy: 50.000 PLN .

Pro zajímavost přikládám ukázky z e-mailů jednotlivých autorů :

A) Článek jsem odevzdal v létě 2007. Po urgencích jsem v prosinci dostal smlouvu. Tu jsem podepsal 17.12.2007. Za měsíc (kdy jsem dle smlouvy měl dostat honorář) jsem se optal na jeho osud. Bylo mi sděleno, že přijde až v únoru.
Pak jsem se ptal v únoru, březnu (to již opakovaně) .
E-maily jsem posílal damám Martyna Zaczek and Sylwia Hacieja.
E-maily jim dorazily, dokonce je i zpočátku četly (přišlo potvrzení), ale již na ně neodpovídají…
Nechal jsem jim i vzkaz na záznamníku.
Dluží mi 5880,- Kč

B) Moje skusenosti s redakciou boli vcelku dobre, ale ked prislo na zmluvy a preplatenie honorara, tak uz to bol problem.
Pisal som znova e-maily pani Zaczek a pani Hacieja, aby ma informovali, preco mi este neprisiel honorar za dalsie clanky.
Obdrzal som uz len e-mail, ktoreho podoba od pani Hacieja je nizsie, ze koncia s vydavanim Hakin9 na ceskom trhu. Odvtedy sa mi uz neozvali a neodpovedaju na e-maily. Mne ako studentovi celkom ide o tie sumy =) dlzia mi este dohromady 10080,-

B) Já mám starou živnost, takže jsem jim vystavoval faktury. Aspoň jsem si to poletech zopakoval. Dokonce jsem je i zdanil. Ale teď jsem se díval do výpisů z účtů a žádnou platbu jsem od nich z poslední doby nenašel. Poslední platba přišla v září loňského roku.

C) Ja som pre Hakin9 napisal clanok do jednoho z jesennych vydani. Oni mi navrhli niekolko sposobov ako mi za clanok mozu zaplatit - pricom ciastocne naliehali aby som im poslal fakturu. Ked som im odpisal ze nie som zivnostnik tak ma poziadali aby som si niekoho zohnal cez koho mi to zaplatia.

D) Nemali absolutne ziadnu snahu nejakym sposobom riesit zmluvy. Az po niekolkych mesiacoch e-mailov a komunikovania, ako by mala zmluva vyzerat, sme sa dohodli na jej podobe.
Potom som znova musel pisat niekolko e-mailov, kym sme sa dostali k tomu, ze mi prve tri zmluvy konecne poslali. Samozrejme podpisal som ich ihned a obratom poslal (to bolo niekedy na konci januara tohto roku).

E) Dohadovali jsem se o způsobu a výši platby. Paní Hacieja mi před napsáním článku slíbila velmi slušný honorář. Po napsání článku jsem se dozvěděl, že suma bude významně nižší. Paní Martyna Zaczek mi řekla, že se kolegyně spletla. No ono je to ve výsledku jedno. Honorář jsem stejně neobdržel…. (cca 5000,- Kč)

Co říci závěrem?

Předpokládám, že všichni dotčení autoři si jména oněch dvou dam a redakce dobře zapamatují a na příště své nadšení publikovat budou korigovat i mnohem přízemnějšími starostmi. Nadále se nebudou starat jen o dodání dobře a včas napsaného článku, ale zjistí si, zda je redakce schopna vystavit autorskou smlouvu, domluví si předem cenu honoráře a případně se pozeptají kolegů na jejich zkušenosti s redakcí. Pak se rozhodnou zda s takovou redakcí budou spolupracovat.

Ve světle předchozích informací, podtitul časopisu *Hakin9 - Jak se bránit?* nabývá úplně jiného významu. Ano, časopis možná některé jedince opravdu naučí „*Jak se bránit*“

Pavel Vondruška
v Praze 15.4.2008

B. MIME formát a NBÚ formát ZEP(ZIP) pre uľahčenie splnenia požiadavky WYSIWYS pri QES

Peter Rybar, NBÚ SK, pr@mailbox.sk

Podpisy patriace do kategórie Qualified Electronic Signature (QES) musia spĺňať niekoľko dôležitých podmienok, z ktorých medzi hlavné patrí požiadavka What You See Is What You Sign (WYSIWYS to, čo vidíš, to aj podpisuješ). Splnenie tejto požiadavky je možné len na základe jednoznačnej identifikácie typu podpisovaného dokumentu takým spôsobom, ktorý neumožňuje neodhaliteľnú zmenu identifikácie typu dokumentu po jeho podpísaní. Príkladom môže byť podpisovanie dokumentov uložených v súbore, kedy identifikácia typu dokumentu je daná príponou súboru. Ak identifikácia typu súboru a teda dokumentu nie je uvedená aj v podpisovaných údajoch, potom je možné identifikáciu typu dokumentu bez odhalenia zmeniť. Z tohto dôvodu podpisové aplikácie, používajúce takúto identifikáciu typu dokumentu, musia používať zložité analyzátory podpisovaného dokumentu. Tieto analyzátory sa snažia na základe analýzy údajov dokumentu určiť pravdepodobnosť, že dokument je daného typu. Útočník môže takéto analyzátory zmiasť falošnými údajmi, ktoré pri jednom type dokumentu môžu byť ignorované, no pri inom type dokumentu zobrazené, a tak zmenou identifikácie typu dokumentu spôsobia odlišné interpretovanie a zobrazenie. Riešením je používanie takých formátov podpisu alebo uloženia podpisovaných dokumentov, ktoré jednoznačne identifikujú typ dokumentu v položkách chránených podpisom podpisovateľa.

Aby takáto identifikácia bola jednotná, kvôli zabezpečeniu interoperability medzi aplikáciami, Národný bezpečnostný úrad (NBÚ) definuje formáty podpisov, podpisovaných dokumentov a uloženia podpisovaných dokumentov do obálky zabezpečujúcej jednoznačnú identifikáciu typu dokumentu.
http://www.nbusr.sk/en/electronic-signature/approved-formats/index.html

Pri bežných implementáciách Advanced Electronic Signature (AdES) je automatickým spôsobom častokrát nezistiteľné, že došlo ku pozmeneniu identifikácie typu dokumentu, lebo štandard AdES chrániť identifikáciu typu iba odporúča, ale nevyžaduje. Odporúčanie však implementácie pre AdES častokrát ignorujú, a tak nedokážu zabrániť realizácii možných podvodov. Produkty, certifikované pre QES, nesmú umožniť chybné zobrazenie dokumentu a musia v každom prípade skontrolovať identifikáciu typu dokumentu, či sa zhoduje so skutočným obsahom dokumentu. Bez explicitného uvedenia identifikácie typu dokumentu je to prakticky veľmi náročné. Napríklad niektoré dokumenty obsahujú textové štruktúry, popisujúce ako sa majú jednotlivé údaje z dokumentu zobraziť, a tak analyzátor typu dokumentu môže iba s určitou pravdepodobnosťou predpokladať, či sa jedná napríklad o TXT dokument alebo dokument iného typu formátu.

Túto nejednoznačnosť riešia MIME typy dokumentov, ktoré pri XML AdES (XAdES) je možné umiestniť do elementu *DataObjectFormat*, ktorý je podpisovaný a tak je chránený podpisovateľovým podpisom proti modifikácii. Ďalším používaným riešením je umiestnenie podpisovaného dokumentu do MIME obálky, kde hlavička MIME obálky obsahuje MIME typ dokumentu a do tela MIME obálky je vložený samotný dokument v kódovaní uvedenom v MIME hlavičke. Podpis MIME obálky potom chráni súčasne MIME hlavičku spolu so zakódovaným pôvodným dokumentom umiestneným v tele MIME obálky.

Riešenie pomocou MIME obálky je užitočné nie len pre CMS AdES (CAdES) ale rovnako aj pre XAdES podpisy. Vzhľadom na obmedzenia vyplývajúce z XML jazyka, je potrebné XML dokumenty pred podpisom kanonizovať (Exclusive XML Canonicalization http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/ alebo http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/, ...), aby sa zabezpečila ich jednotná binárna forma pred podpisom. Podľa typu použitej kanonizačnej funkcie sú z XML dokumentu odstránené rôzne znaky alebo komentáre a podpisom je tak chránená iba časť pôvodného dokumentu, ktorá je jednotná pre všetky aplikácie, obsahujúce korektne implementovanú kanonizačnú funkciu. Pri použití MIME obálky alebo BASE64 kódovaní podpisovaného dokumentu nie je potrebné použiť kanonizáciu na podpisovaný dokument, čo ušetrí značné množstvo času a systémových prostriedkov na analýzu a výslednú kanonizáciu dokumentu pred podpisom a pri overovaní podpisu dokumentu.

Ďalšou výhodou pri podpisovaní MIME obálky je zabezpečenie interoperability nielen medzi aplikáciami vytvárajúcimi XAdES či CAdES, ale aj medzi XAdES a CAdES navzájom, lebo podpisovaný je vždy rovnaký binárny súbor, a tak je možné vytvárať viacnásobné podpisy toho istého dokumentu bez obavy, či je použitá rovnaká kanonizácia pri XAdES.

Ďôležitou otázkou pri používaní podpisov je možnosť viacnásobného podpisovania dokumentu s viacerými podpisovateľmi podpisujúcimi fyzicky na navzájom vzdialených miestach. CAdES takéto podpisovanie rieši priamo v svojej definícii, no XadES, vzhľadom na jeho implementáciu pomocou XML jazyka, takéto niečo neumožňuje alebo len obmedzene. Je to kvôli obmedzeniu XML jazyka, ktoré požaduje jedinečné identifikovanie elementov v jednom XML dokumente, a tak výsledné XML nemôže byť poskladané z XML podpisov vytvorených viacerými podpisovateľmi nezávisle na sebe, lebo tieto XML podpisy obsahujú identifikátory XML elementov s rovnakými hodnotami, čo v XML jazyku nie je prípustné a zmena identifikátorov nie je možná, lebo by sa tým porušil samotný podpis. Aj pre vyriešenie tohto problému s XAdES viacnásobným podpisom a pre dosiahnutie kompatibility s CAdES podpisom NBÚ navrhlo formát ZEPf (ZIP) pre vytváranie „detached" typu podpisu, čo znamená, že podpisovaný dokument a podpis sú v samostatných dokumentoch. Ak ku tomu ešte pridáme užitočnú požiadavku na uloženie dokumentu do MIME obálky, získame tak interoperabilný podpis umožňujúci viacnásobné podpisovanie. A samozrejme ako užitočný vedľajší efekt, vďaka použitiu ZIP algoritmu, získame ľahko prenositeľný balíček so skomprimovaným podpisom a dokumentom.

Ak nevyžadujeme kompatibilitu CAdES podpisu s XAdES podpisom a veľkosť dokumentu nám neprekáža, môžeme namiesto ZEP formátu použiť S/MIME formát na uloženie CAdES podpisu a dokumentu, čím získame podpis overiteľný vo veľkom množstve e-mail programov.

Ak si chcete vyskúšať vyššie spomenuté formáty podpisu a uloženia podpisu do ZEPf(ZIP) alebo S/MIME formátu, môžete použiť pripravovanú FREE aplikáciu ELPI2, dostupnú na adrese http://elpi2.szm.com/ , ktorá vytvára CAdES podpis pomocou smart karty komunikujúcej cez rozhranie PKCS11 alebo pomocou súborového tokenu PKCS15. Táto aplikácia je zatiaľ v pracovnej alfa verzii, a tak niektoré jej časti ešte nie sú úplne odladené. Prípadné návrhy na doplnenie alebo zistené chyby môžete zaslať na pr@mailbox.sk a v najbližšom čase môžu byť doprogramované. Kľúče a certifikáty si môžete vygenerovať v staršej verzii http://elpi.szm.com/ .

C. Trusted Computing

Petr Sušil, MFF UK, susil.petr@gmail.com

Úvod

Trusted Computing Group (TCG) [1], dříve Trusted Computing Platform Alliance (TCPA), je organizace, jejímž úkolem bylo vyvinout standardy pro trusted computing. TC specifikace splňuje Evaluation Assurance Level 3 podle Common Criteria ISO/EIC 15408, Protection profile a certifikát lze nalézt v [2].

Proč používat Trusted Computing [3]

Stefik definuje důvěryhodný systém jako systém, který vždy pracuje podle stanovených pravidel (čtenář může nalézt původní definici v [4]). Většině současných systémů nelze vůbec důvěřovat. Viry a trojské koně jsou používány při krádežích soukromých informací a provádění denial of service útoků. Vylepšování současného software nemůže tento problém vyřešit, neboť libovolné softwarové řešení je zranitelné vůči softwarovým útokům. Platformy založené na trusted computing budou méně zranitelné vůči softwarovým a hardwarovým útokům a umožní tak lepší ochranu uložených dat a poskytovaných služeb.

Máme-li jak hardwarovou tak softwarovou podporu, můžeme vynutit dodržování libovolných pravidel a omezení. Např. demo písničky povolíme přehrát na každém systému pouze jedenkrát.

Samozřejmě ale nemůže kontrolovat, zda si uživatel nevytvoří vlastní kopii (se ztrátou kvality) při přehrávání. Podobný přístup může být použit i na libovolný dokument. Pokud bychom používali TC-office, potom libovolný dokument vytvořený v TC-office může být zobrazen jen tímto softwarem či softwarem certifikovaným výrobcem, který tak může vytvořit monopol. Pokud nebude mít uživatel software kompatibilní s TC-office, nebude moci přečíst žádný dokument vytvořený tímto software. Například právní kancelář by poté musela vlastnit mnoho různých kancelářských balíků, aby mohli přečíst maily a dokumenty všech svých klientů.

Kritéria návrhu nejsou veřejně známá. Dochází k přesunutí kontroly od uživatele k výrobci software, a tedy může docházet k cenzuře. Proto někteří překládají zkratku TC jako Treacherous Computing [5].

Mechanismy Trusted Computing

TCG vytvořilo specifikaci [6] pro hardwarový čip zvaný TPM (Trusted Platform Module). Tento čip je základním stavebním kamenem, na němž je založena (softwarovou) bezpečnost lokálního systému a autentizace vzdáleného systému (důkaz, že vzdálený operační systém je též důvěryhodný).

Dnešní operační systémy bohužel nejsou vůbec důvěryhodné. Jádro OS je příliš velké na to, aby bylo možné ověřit, zda neobsahuje bezpečnostní slabiny, a navíc by šlo o plýtvání časem, neboť jich vzhledem k rozsahu kódu pravděpodobně obsahuje mnoho – to platí jak pro Linux, tak pro Windows. Běžně používané OS jsou monolitické, což znamená, že jádro má právo k provedení libovolné operace [7]. To je též bezpečnostním rizikem, neboť bychom chtěli vždy přidělovat jen potřebná práva. Vytvoření takového jádra by však bylo příliš nákladné, a navíc by vzniklé jádro muselo projít dlouhým testováním, než bychom dosáhli stejné bezpečnosti jako ve stávajících OS. Proto je potřeba nalézt řešení, které funguje i pro stávající (monolitické) OS. Předpokládejme, že OS je dostatečně bezpečný, ale má nějaké bezpečnostní slabiny, kterých může útočník využít. Útočník může poté změnit aplikaci či její konfiguraci a převzít tak kontrolu nad systémem. Pokud dokážeme detekovat takovou změnu, pak můžeme

důvěřovat i nezabezpečenému OS. K tomu slouží bezpečné bootování spolu s detekcí změny konfigurace (od posledního naběhnutí systému) – protokol, který umožňuje zjistit změnu v konfiguraci, je uveden v [9].

Bezpečné bootování [3, 9]
Předtím, než BIOS předá kontrolu OS, existuje velký prostor pro útok. Abychom předešli takovým útokům, ověříme celý bootovací proces tím, že každý blok použitý při bootování je předán TPM pro výpočet kontrolního součtu. TPM při nesprávném součtu bootovací proces zastaví. Protože neexistuje jiný způsob jak nastavit tuto hodnotu v TPM, lze se takto ujistit, že před nabootováním OS nebyl žádný aktivní virus nebo trojský kůň. Poté už se plně spoléháme na OS, že nemá žádné slabiny, které nemůžou být přímo zneužité. Kontrolní součet může být též využít k otevření externího úložiště klíčů.

Vzdálené osvědčení [9]
Dalším problémem, který trusted computing řeší je rozsáhlá počítačová síť. Abychom měli zabezpečenou počítačovou síť, musí být každý počítač, který je její součástí, také zabezpečený. Pokud chceme poslat citlivá data na jiný počítač, musíme se nejdříve ujistit, že cílový počítač je též dostatečně zabezpečený. Pokud není firemní bezpečnostní politika dostatečně přísná (např. žádný internetový přístup, žádná vstupně/výstupní mechanika atd.), pak neexistuje žádná možnost jak toto zabezpečení zkontrolovat s dostatečnou jistotou, neboť může obsahovat virus či trojský kůň, který ještě nebyl detekován, nebo systém nemusí být bezpečný sám o sobě (disk není šifrovaný, neboť tato funkce byla vypnuta). Stručně řečeno je potřeba získat vzdálené osvědčení. Takové osvědčení nemůže být zajištěno pouze softwarem, neboť by takové řešení bylo zranitelné vůči softwarovým útokům. Důvěryhodný hardware zná stav systému a může se identifikovat (dokázat, že je důvěryhodný). Stav je získán při bezpečném bootování a identifikace je provedena pomocí TTP, nebo přímo pomocí anonymous attestation protocol (důkaz s nulovou znalostí) [8]. Použití TTP není dostatečné pro větší množství serverů a DAA protokol je velmi komplikovaný. Přímý důkaz identity není možný kvůli ochraně soukromí [9]. Vzdálené osvědčení umožní detekovat změny v předchozí konfiguraci. Buď dochází k posláním všech konfiguračních parametrů, nebo se používá osvědčení pro jednotlivé parametry, je-li prozrazení nevyžádaných informací narušením soukromí.

Oddělení jednotlivých procesů [7]
Je též rozumné oddělit jednotlivé procesy běžící na dané platformě, neboť některý proces může být špionážní (například útok postraním kanálem na implementaci RSA – kdy je možné získat klíč pouze na základě cache-miss v podepisovacím algoritmu).

BitLocker [10, 11]
Výhody laptopů jsou nepopiratelné a pravděpodobně budou za několik let používanější než desktopy. Firemní laptopy často nesou citlivé informace a jsou velmi často předmětem krádeží nejen kvůli ceně zařízení ale hlavně kvůli informacím, které obsahují. Staré pevné disky obsahující citlivé osobní údaje jsou běžně k dostání v bazarech [9]. Pokud je nabootován jiný operační systém než je nainstalovaný na příslušném disku, je možný přístup ke všem souborům a to i pokud instalovaný operační systém omezuje přístup k daným souborům a útočník by tedy po jeho nabootování přístup získat nemohl. Naším cílem je ochránit citlivé informace, i pokud má útočník neomezený přístup k laptopu a jeho pevnému disku. Uživatel vždy může šifrovat citlivé informace své pomocí, nicméně to není dostatečně pohodlné, což je důvod proč většina citlivých dat zůstává nešifrovaná. Navíc tento postup částečně selhává, neboť citlivá data mohou být uložena na disku i ve volném místě či ve swapu. Rozlišení mezi

citlivou a běžnou informací navíc nemusí být zcela zřetelné. Pro vyřešení těchto problémů je možné použít šifrovaný filesystem. Pak ale musí uživatel vkládat heslo při každém startu počítače, což je pro většinu uživatelů stále příliš nepohodlné. Běžný uživatel proto tuto funkci vypne – běžný uživatel není ochoten podniknout žádný dodatečný krok k zajištění vyšší bezpečnosti. Je-li v počítači instalovaný TPM modul, pak může být využit k ochraně šifrového klíče pevného disku, a uživatel jej nemusí ručně zadávat. Poté co je systém nastartován z nezabezpečené jednotky, obsahuje TPM hash posloupnosti bloků použitých pro start systému. Pokud je nastartován správný a nezměněný operační systém (OS nebo jeho konfigurace nebyla změněna), pak šifrový klíč je uvolněn a použit pro přístup k jednotce. Jak si čtenář jistě povšiml, žádná akce od uživatele nebyla potřeba (nicméně bezpečnost může být dodatečnou akcí uživatele zesílena – PIN/USB disk). Pokud není v systému TPM přítomen, pak musí být heslo zadáno vstupem z klávesnice nebo USB disku.

BitLocker provádí šifrování na úrovni sektorů, což znamená, že filesystem o šifrování disku neví. Navíc to znamená, že šifrový text a otevřený text musí mít stejnou délku. Vzhledem k tomu, že BitLocker je komerční řešení má výkon přednost před bezpečností. Šifra BitLocker se skládá z AES v Cipher Block Chaining (CBC) módu a Elephant diffuseru.

Proč AES, CBC a diffuser?
Předpokládejme, že jsme útočník a získali jsme laptop s TPM s zašifrovaným diskem bez dalšího zesílení bezpečnosti. Lze nastartovat přítomný operační systém a tím jednotku dešifrovat, nicméně tím nezískáme přístup k citlivým datům z důvodu restrikcí OS. Nicméně se můžeme pokusit vytvořit v OS slabiny, které umožní získat superuživatelský přístup. Stačí tedy vytvořit kód v assembleru a zkopírovat jej do jádra OS. To však nelze provést přímo, neboť operační systém obsahuje kontrolu přístupu. Nelze to provést ani v jiném OS, neboť je disk šifrovaný. Vytvoříme tedy kód v instalovaném OS, abychom získali zašifrovanou verzi a poté jí přesunout na místo jádra instalovaného OS. Tento přístup by fungoval, kdyby byl každý sektor šifrovaný stejně (Electronic Code Book mode). Proto BitLocker musí autentizovat data čtená z disku. Nicméně pro autentizační informace není na disku žádné místo. Pokud neexistuje uvedená slabina, pak útočník nemůže o otevřeném textu nic předpokládat ("poor-man authentication"). Pak při přesunu našeho kódu na jiný sektor bude kód pravděpodobně neplatný a OS spadne bez poskytnutí přístupu k souborům.

Chceme-li předejít kopírování dat z jednoho sektoru na druhý, existuje standardní řešení - CBC mód kdy chaining value odvodíme z čísla sektoru. Ale CBC mód má také slabiny. Při zavedení diference
Δ v bloku *i* šifrového textu se projeví jako diference Δ v bloku *i+1* otevřeného textu [12] a podobný útok může být využitý k rozbití poor-man authentication a měnění souborů známým způsobem. Elephant diffuser právě řeší tento problém [11, 12]. Nyní je potřeba zvolit šifru dostatečně rychlou jak v hardware tak software, bezpečnou a veřejně posuzovanou – bylo zvoleno AES.

Šifra BitLocker je kompromis mezi bezpečností a rychlostí [11]. AES je standardizovaná bezpečná šifra, CBC mód zabraňuje přesouvání dat mezi jednotlivými sektory disku a Elephant diffuser spolu s CBC zabraňuje předvidatelným změnám při těchto přesunech. Elephant diffuser není veřejně posouzený, ale neoslabuje bezpečnost AES, a tedy je BitLocker alespoň tak bezpečný jako AES in CBC módu [11].

Microsoft vybíral mezi rychlostí a bezpečností a rychlost byla na prvním místě. Šifra BitLocker byla navržena pro 3GHz P4. Na pomalejších PC může být překážkou a systém

zpomalovat. Model útočníka pro BitLocker je nestandardní model – jeho popis může čtenář nalézt v [11]. Pokud se podaří uskutečnit obecnější útok, pak je pravděpodobné prolomení šifry (pravděpodobně poor-man authentication).

Literatura:

[1] "Trusted Computing Group." www.trustedcomputinggroup.org/
[2] "Common Criteria Evaluation and Validation Scheme." www.niap-ccevs.org/cc-scheme/pp/PP_TCGPCTBB_V2.5-VR.pdf www.niap-ccevs.org/cc-scheme/pp/PP_TCGPCTBB_V2.5-CI.pdf [Accessed Aug. 28, 2007]
[3] S. Pearson, "Trusted Computing: Strengths, Weaknesses and Further Opportunities for Enhancing Privacy," in *Trust Management*, vol. 3477/2005, *Lecture Notes in Computer Science*. Heidelberg: Springer Berlin, 2005, pp. 305-320.
[4] D. K. a. R. A. Gehring, "Trusted Platforms, DRM, and Beyond," in *Digital Rights Management*, vol. 2770/2003, *Lecture Notes in Computer Science*. Heidelberg: Springer Berlin, 2003, pp. 178-205.
[5] R. Anderson, "Cryptography and Competition Policy - Issues with 'Trusted Computing'," in *Economics of Information Security*, vol. 12, *Advances in Information Security*: Springer US, 2004, pp. 35-52.
[6] "TCG Specification Architecture Overview, Specification Revision 1.4, 2nd August 2007. www.trustedcomputinggroup.org/groups/TCG_1_4_Architecture_Overview.pdf [Accessed Aug. 27, 2007]
[7] K. K. a. C. Wolf, "Trusted Computing, or the Gatekeeper," in *IFIP International Federation for Information Processing*, vol. 195/2006. Boston: Springer Boston, 2006, pp. 339-354.
[8] S. X. Hao Liming, Yang Shutang, and Lu Songnian, "A method to implement full anonymous attestation for trusted computing platform," *Wuhan University Journal of Natural Sciences*, vol. Volume 12, Number 1 / January, 2007, pp. 101-104, 2007.
[9] K. Kursawe, "Trusted Platforms," in *Security, Privacy, and Trust in Modern Data Management, Data-Centric Systems and Applications*. Heidelberg: Springer Berlin, 2007, pp. 119-131.
[10] Z. Bowden, "Using BitLocker in a Higher Education Environment," 2007. http://tmig.w2k.vt.edu/docs/BitLocker_in_HigherEd.pdf [Accessed Aug. 20, 2007]
[11] N. Ferguson, "AES-CBC + Elephant diffuser A Disk Encryption Algorithm for Windows Vista," Microsoft, 2006. http://download.microsoft.com/download/0/2/3/0238acaf-d3bf-4a6d-b3d6-0a0be4bbb36e/BitLockerCipher200608.pdf [Accessed Aug. 21, 2007]
[12] D. MacIver, "Penetration Testing Windows Vista BitLocker Drive Encryption Penetration Testing Windows Vista," 2006. http://conference.hackinthebox.org/hitbsecconf2006kl/materials/DAY%202%20-%20Douglas%20MacIver%20-%20Pentesting%20BitLocker.pdf [Accessed Aug. 23, 2007]
[13] M. Z. David Safford*, "Trusted computing and open source," 2005. http://infosec.pku.edu.cn/~caozhen/courses/readings/11.2.pdf [Accessed Aug. 23, 2007]

D. Ještě o Dr. Rafaelovi
Jan B. Hurych

V minulém článku, "ZÁHADNÝ DR. RAFAEL" jsem se snažil shromáždit více informace osobě, která prý "znala" historii původu VM. Zde půjdeme ještě dál, . . .

Role, kterou Dr. Mnišovský hraje v historii původu rukopisu VM, je kritická. Jak Marci nepřímo přiznává, informace, kterou od něj dostal, jsou pravděpodobně jen dvorní klepy a Marci se osobně za ně nezaručuje. Je to divné, protože na druhé straně se neváhal ve svých jiných dopisech zaručit za Barešovu osobu, ale to byl člověk, kterého znal velmi dobře. Ve své knize "Philosophia vetus restituta" dokonce prohlašuje, že Bareš byl jeho přítel a z posledního dopisu je cítit jeho sympatie s člověkem, který strávil poslední léta svého života řešením VM. Marci ve svém dopise také uvádí, že spolu s rukopisem posílá i poznámky od Bareše. Zatím tomu nikdo z výzkumníků nevěnoval pozornost. Co se s nimi asi stalo, pane Voynich? Pokud si teda Kircher uschoval i dopis, proč ne poznámky?

Co se týká Mnišovského, Marci ho uvádí spíše jako známého a radí Kircherovi, aby se "sám rozhodl, čemu věřit". Pokud si teda Marci ještě 22 let po Mnišovského smti pamatoval tu informaci dobře, máme zde stále ještě dva problémy:

1) *Byla Mnišovského informace založena na faktech nebo ne?*

2) *Řekl Mnišovský Marcimu celou pravdu?*

Tímto si i rozdělíme hlavní otázku na dvě, hlavně proto, že někteří výzkumníci tvrdí, že tyto „klepy“ jednu dobu kolovaly u císařského Dvora (kupodivu ale o tom nikde jinde zprávu nenalezneme) a že tedy Mnišovský opakoval jen to, co slyšel, ale sám nezažil. Druzí se domnívají, že měl nějakou soukromou, tajnou informaci, kterou znalo jen pár lidí. A jiní dokonce tvrdí, že si to vše Mnišovský jen vymyslel.

1) Předpokládejme tedy nejprve, že Mnišovský opakoval přesně a že dvorská šeptanda byla založena jen na faktech - ale pak bychom ovšem za posledních sto let intenzivního hledání museli někde najít o ní ještě nějakou zmínku. Nic z toho se nestalo, ani Dee ani Sendivogius či jiný pražský alchymista, astronom nebo historik, nikdo z nich se VM ani nezmiňuje! Pouze prof. Newbold, 300 let později, si zopakoval Mnišovského dohad o Baconově autorství a vyrobil kolem něho celé "řešení". Tím tomu ale udělal špatnou službu, protože po Newboldově smrti se zjistilo, že celé jeho řešení je nesmysl, který nelze ani ověřit. Pravda, Mnišovského historka o 600 dukátech se nápadně podobá té o 630 dukátech v deníku Johna Dee, ale tam vůbec neříká nic o prodeji, darování nebo dokonce jak vlastně k penězům přišel. Jinak puntičkářský John Dee prostě nedává žádná jiné detaily, ani to, jak k této sumě vůbec přišel. Navíc měl u sebe celou řadu rukopisů a sotva by se rozloučil zrovna s VM, který byl jistě ten nejzáhadnější a nejzajímavější.

Jestliže teda Mnišovského historka nebyla nikde dokázána, můžeme tvrdit, že neplatí? Ne tak rychle, víme jen, že jsme se octli v mrtvém bodě. Podobně nevíme ani nic o Horčického vlastnictví, vyjma jeho jména ve VM, které se kdysi "zázračně" objevilo Voynichovi. Jméno, které není ani psáno jeho rukou (viz můj článek "NÁŠ OBJEV PODPISU"). Jméno, které za

posledních sto let zase pomalu mizí, díky nešťastné a nesmyslné Voynichově aplikaci neznámých chemikálií.

2) Druhá otázka je ještě složitější: nevíme, zda Mnišovský lhal anebo ne. Dvorní klep mohl existovat přesně tak, jak ho vypověděl Marcimu, ale na to máme jedině slovo Mnišovského, a jak víme, byl také povoláním právník :-). Ovšem pokud je historka pravdivá (tj. otázka č.1 byla zodpovězena kladně), máme ještě pořád jen jeho verzi. Marci neříká, že to slyšel ještě někde jinde, a proto se asi také nechtěl za historku zaručit.

Zkusme to tedy z druhého konce: řekl to Mnišovský i ještě někomu jinému? Zatím o nikom takovém nevíme. Marci se o nikom nezmiňuje a Bareš dokonce ani o té historce nepíše. Takže jsme i zde opět v mrtvém bodě. Mohli bychom si ovšem položit další řadu otázek. Například zda to Mnišovský řekl Marcimu jen tak mimochodem mezi řečí nebo to naopak byl Marci, který se na to Mnišovského sám tázal? Oba byli členové císařského dvora, oba měli vysoké funkce (Marci byl hlavní lékař českého království) a dá se očekávat, že koridory pražského hradu se jen hemžily různými dvořany, kteří neměli nic lepšího na práci než si říkat drby. Ale pokud se ho Marci sám ptal, jak vlastně přišel na to, že má ptát právě jeho? Zřejmě věděli o svých kryptografických zájmech: Marci jednou s Kircherem řešil tajnou šifru švédského generála Bannera a Mnišovský (jak nyní víme) dokonce napsal učebnici tajného písma.

Je možné, že někdo Marciho k Mnišovskému poslal, aby se ho zeptal, zda o tom něco neví? Ano, uhodli jste, mohl to být sám Bareš. V tom případě asi ale také i on musel vědět o Mnišovského zájmech či o jeho knize. Zde je ovšem velký prostor pro spekulaci a Wikipedia dokonce tvrdí, že Bareš dostal VM přímo od Mnišovského. Navíc ještě tvrdí, že VM napsal sám Mnišovský jakožto podvrh. Ovšem Bareš zřejmě neřekl Marcimu, odkud VM má, jinak by to ten určitě napsal Kircherovi, alespoň v dopise, který mu poslal společně s VM.

Zatím se ale věnujme jen faktům. Když Mnišovský dává Marcimu historku jaksi "k dobru", měl už tehdy Bareš VM ve vlastnictví? Ve své knize, vytisknuté roku 1662, Marci tvrdí, že už zná Bareše 40 let. Podle známého luštitele VM René Zandbergena, Marci znal Bareše patrně už od dříve, před rokem 1622, možná od roku 1618, kdy začal studovat v Praze, ale tehdy ještě nebyli přátelé. Také Horčický byl tehdy ještě na živu (zemřel 1622) a je možné, že vlastnil VM až do své smrti. Pokud vůbec kdy VM měl, zatím máme jen jeho jméno ve VM, které někdo vymazal patrně ještě před Barešem, nebo dříve, protože si ho nevšimli ani Bareš ani Marci. Ovšem Horčický byl uvězněn v roce 1618 Direktoriem, později vyměněn za Dr. Jesenia (kterého věznili císařští) a poslán do exilu. Po bitvě na Bílé hoře se vrací, aby za rok na to zemřel. V knize *Historie česká* (napsaná 1626) píše Pavel Skála ze Zhoře, že byli domy katolických exulantů vydrancovány. To by naznačovalo, že pokud VM s sebou nevzal do vyhnanství, pak se VM "ztratil" právě tehdy. V roce 1625 Marci promoval na doktora medicíny a hned v roce 1626 byl jmenován Hlavním lékařem českého království, patrně proto, že byl jeden z prvních lékařů, které vyprodukovala nová fakulta lékařství Karlovy univerzity a díky jisté protekci (jeho známí byli hrabě Lobkowitz a arcibiskup Harrach); tím se stal automaticky i členem císařského Dvora. Později se stal i osobním lékařem Ferdinanda III. a Leopolda I. Mnišovský byl ovšem členem Dvora od roku 1618.

Bareš napsal první dopis Kircherovi již v roce 1637 a poslal jej po páteru Moretovi, který zrovna cestovala do Říma. To znamená, že nejen VM v té době vlastnil (poslal s ním i ukázky z VM), ale pravděpodobně ho získal ještě dříve, uvážíme-li, že jistě váhal, nejprve zkusil řešení sám, pak se ptal známých a možná i Marci mu už v té době pomáhal VM řešit. Podle dohadu některých výzkumníků jej k zaslání inspirovala Kircherova kniha *Prodomus Coptus*

(1636), kde Kircher luštil neznámá písma. V roce 1638 dokonce Marci sám cestoval do Říma a potkal se s Kircherem, ovšem ne kvůli VM. Ve stejné době už sice věděl, že Bareš má VM, ale nevíme, zda o tom s Kircherem mluvil. Tak či tak Kircher na první dopis Bareše neodpověděl. To víme z jeho druhého dopisu, který mu v roce 1639 píše Bareš a který se zachoval. Takže Bareš získal VM asi někdy mezi 1622 (kdy Horčický umírá) a 1637 (kdy píše Kircherovi první dopis). V celé té době se už znali s Marcim velmi dobře. Zdá se, že Bareš patrně nedostal rukopis o mnoho dříve, než se Marci stal členem dvora (1626). Kdy to bylo asi poprvé, kde se Marci a Mnišovský setkali u Dvora a mohl se ho zeptat) a nejpozději asi 11 let později, 1637 (kdy jak už víme, rozhodně VM měl). Ovšem soudě podle toho, že Bareš byl asi nedočkavý, aby řešení získal, nečekal by celých 15 let, než by zkontaktoval Kirchera.

Marci tvrdí, že informaci dostal od Mnišovského osobně (píše "řekl mi"). Předpokládejme, že se ho Marci na to přímo otázal - patrně na naléhání Bareše. Ta konverzace se mohla dít mezi 1626 (Marci prvně u Dvora) a 1644 (kdy Mnišovský umírá). Řekněme tedy, že Bareš dostal VM v roce 1626 a když se nic víc nedozvěděl od Mnišovského, napsal Kircherovi první dopis (1637). To by ale stále ještě čekal 11 let, i když věděl, že Marci Kirchera zná. Od kdy ale vlastně Marci Kirchera znal? Podle dopisů Kircherovi v *Museo Kircheriano*, první dopis Kircherovi je datován z roku 1640, ten samý rok, co uviděl Kirchera v Římě. V něm zve Kirchera k pražskému Dvoru a ještě stejný rok mu už doporučuje Bareše (patrně aby mu nenápadně připomněl, že Barešovi neodpověděl ani na druhý dopis z roku 1639). Anebo odpovídá na dotaz od Kirchera, který už měl druhý dopis od Bareše a chtěl vědět, zda se nejedná o podvrh. Vzbudil v něm snad druhý dopis větší zájem nebo to psal Marci zase jen na naléhání od Bareše? V té době asi měl Bareš pořád ještě velké naděje, že rukopis rozluští, takže to bylo asi nějak brzo po získání rukopisu než později, i když to - podle Marciho - nikdy nevzdal. Pokud tedy Bareš dostal VM někdy kolem roku 1635 či později, chybí nám fakta o době mezi 1622 (smrt Horčického) a 1635, teda nejméně 13 let...

Odborník na Kircehrovu tvorbu, *J. Fletcher* se zmiňuje o tom, že Bareš byl jednou sám v Itálii, aby navštívil Kirchera. Bohužel tato informace není potvrzena, jedná se patrně o Marciho, nebo o to, že Bareš v Itálii studoval. To ale bylo daleko dříve, než tam vůbec přišel Kircher z Německa učit. Může také to být důvod, proč se Marci v dopise Kircherovi nezmiňuje o Barešovi jménem? Asi ne, v dopise Kircherovi naznačuje, že mu už Bareš předtím psal. Můžeme usoudit, že pokud se Kircher zajímal o VM (a to jako řešitel tajných písem asi ano) pak se asi snažil ignorovat kopie od Bareše a místo toho chtěl do rukou originál. Bylo by to logické, protože individuální vzorky by mu moc neřekly a také byl nepochybně podezíravý, že jde o podvrh (už jednou předtím Kirchera někdo napálil). Bareš, mu ovšem zřejmě nechtěl rukopisu přímo předat, chtěl si uchovat obsah, ono tajemství, jen pro sebe, patrně kvůli finančnímu zisku. Jenže bez celé knihy neměl Kircher šanci a tak viděl, že ho chce Bareš zneužít a odmítal sloužit takovému účelu. Bareš si patrně ani nepřál, aby po jeho smrti Marci VM poslal Kircherovi, jinak by mu rukopis poslal už sám. Zdá se, že i Marci váhal (možná až čtyři roky!), než VM Kircherovi poslal, protože Bareš patrně umřel už před rokem 1662.

Ale vraťme se k Mnišovskému. Svou knihu o kryptografii dokončil v roce 1628 - z toho asi plyne omyl ve Wiki, že se v roce 1618(!) chlubil, že vynalezl neřešitelnou cifru. To totiž, jak jsem zjistil, sám prohlásil právě v předmluvě k této knize. Nehledě na to, že šifra v knize není neřešitelná :-). Je rok 1628 jen o dva roky později než s ním mohl Marci u Dvora vůbec mluvit. V té době by asi také - nejpravděpodobněji - Bareš knihu získal. Druhá možnost, že ji Bareš dostal hned po smrti Horčického, by znamenala, že by Marci musel ještě 4 roky čekat, než by mohl mluvit u Dvora s Mnišovským, pokud se teda neznali od dříve - ale jak, když

Marci byl do té doby jen obyčejný student. A navíc by Bareš musel napsat svůj dopis Kircherovi až po 17 letech od získání VM. Nezdá se pravděpodobné, že by vydržel tak dlouho čekat, soudě podle toho, jak si usilovně přál řešení najít a jak zřejmě pořád na Marciho tlačil, aby jej u Kirchera urgoval!! Jenže dostal-li knihu později, kdo ji měl celou tu dobu po Horčického smrti? Možná Jezuité, kterým Jacobus téměř vše ve své závěti odkázal, ale jak by ji od nich Bareš získal? Pravda, považovali by asi VM za jednu ze zakázaných knih, tzv. Libri prohibiti. Oni ovšem pálili jen laciné výtisky knih zabrané u obyvatel, ty cennější nepálili, ale schovávali a zamykali do archivů :-).

Nejpravděpodobněji dostal Bareš knihu prostě od někoho jiného než od Jezuitů. Ano, mohl ji dostat od Mnišovskébo, proč ne? Ten ji mohl mít nějakou dobu u sebe, ale od koho ji dostal on? Pravda, oba byli s Horčickým zavilí katolíci, ale Jacobus byl tak přímo vychován Jezuity, kterým jako chudý chlapec vděčil za vše, zatímco Rafael si jen vylepšoval kariéru. I na epitafu, který si sám předem napsal, netvrdí, že sloužil Bohu, ale císaři. Kromě toho, jeho kariéra začala vlastně až v roce 1622, nemohl už teda znát ani Horčického ani Bareše nějak moc dobře. Jedno je jisté: ani Mnišovský, ani Bareš neřekli Marcimu plnou pravdu, pro nám dosud neznámé důvody. Tak např. Bareš se mu nesvěřil odkud VM má, jinak by to Marci Kircherovi napsal - ve svých dopisech mu vždy upřímně psal vše co věděl. Navíc z Barešova dopisu Kircherovi cítíme jistou neupřímnost. Sotva lze totiž věřit, že chtěl VM vyluštit je pro "blaho lidstva" a dobře víme, že neříká pravdu, když tvrdí, že mu kniha "jen zabírá na regále místo a hromadí se na ní prach". Marci naopak popisuje, s jakou vášní se Bareš VM věnoval. Mnišovský zase Marcimu neřekl odkud ví, že Rudolf II. vlastnil *právě tento* rukopis. Je tu ovšem ještě jedna možnost, proč Mnišovský neřekl vše . . .

Ocitujme z anglické **Wikipedie**: Mnišovský...*"přítel Marciho, který je údajným zdroje historky o Baconvi, byl sám kryptograf (mimo jiné) a zřejmě vymyslel šifru, o které tvrdil, že je nerozluštitelná (asi 1618). To vede k teorii, že on sám vyrobil VM jako praktickou ukázku jeho šifry - a z Bareše si udělal pokusné morče. Když Kircher publikoval svoji knihu "Prodomus Coptus", Mnišovský si možná pomyslel, že jej bude cennější pokořit Kirchera než Bareše a přesvědčil ho, aby požádal Kirchera o pomoc. K tomu si vymyslel historku o Baconovi, aby Bareše motivoval. Marci ve svém dopise naznačuje, že historce nevěří. Ovšem nemáme žádný důkaz pro tuto teorii (konec citátu, zdroj informace neuveden, j.h.)*

Snažil jsem se nějakou dobu najít autora citátu, ale marně. Kdokoliv to ale byl, měl uvést, že nejprve se o této domněnce zmiňuje Jorge Stolfi (ve VM Listu, msg00052.html, 27 Dec 2000) není to sice přesně totéž co je uvedeno ve Wikipedii, ale už zde také podezřívá Mnišovského z podvrhu. Nebudeme se zde snažit ověřovat či popírat uvedené tvrzení, protože citát sám jasně mluví jen o teorii a nedostatku důkazů. V poslední době jsem si však ověřil tři nová fakta, která dělají z uvedené teorie opravdovou možnost.

První objev

Je fakt, že Mnišovského kniha "**Construction sive strues Trithemiana**" (1628) není žádná učebnice češtiny, jak se dosud tvrdilo, ale opravdová kódovací kniha ve stylu Trithemia, jak sám autor přiznává. Díky mému známému (českému kryptologovi *Mgr. P. Vondruškovi)* můžeme teď s jistotou říci, že se jedná o šifru, kterou Mnišovský sám vynalezl (viz můj předešlý článek "ZÁHADNÝ DR. RAFAEL". Šifra je ve stylu "Ave Maria" (šifrového systému, který popsal Thrithemius). Používá však hned dvě verze kódu, českou a latinskou. Nahrazuje jako Ave Maria každé písmeno originálního textu jedním celým slovem, ale s 24 variantami. Zašifrovaný text pak vypadá jako nevinný dopis v češtině (či latině). Zatímco Trithemius používá jen slova z modliteb, Mnišovský vybírá slova z denního života a rozděluje je podle gramatického klíče. Tak např. písmeno A je nahrazeno vždy jen přídavným jménem.

(Poznámka: používám zde slovo *kód* a *šifra* zcela volně, ne tedy zrovna přesně podle definice. Ale kódu "Ave Maria" se například všude říká *šifra* a přesto vyloženě používá slova z kódovacího seznamu :-)).

Abych si potvrdil mé podezření, hledal jsem dále a dostal jsem velice cennou informaci od skvělého slovenského odborníka *Mgr. Jozef Krajčoviče, PhD.*, který mi laskavě dodal citáty z knihy **Kašpar, J.: Soubor statí o novověkém písmu** (The Compendium of Articles about the Modern History Writings, Praha, Karolinum 1993. ISBN 80-7066-679-X. str. 188-190, *Kapitola 6., The Secret Writings in Modern History*. (Tajná písma z moderní historie). Můj překlad nebude asi zcela přesný, je to z angličtiny zpět do češtiny, ale doufám, že jsem zachoval podstatu:

*"První česká učebnice kryptologie je ručně psaná kniha **Constructio sive Strues Trithemiana**, napsaná v roce 1628 českým právníkem a vysokým císařským úředníkem Rafaelem Soběhrdem - Mnišovským ze Sebuzína a Horštejna, založená na stejném principu jako je Trithemiova Polygraphia. Liší se ve dvou bodech: je dvojjazyčná, tj. česko-latinská a podle autorových slov v úvodu má sloužit nejen jako kryptologická učebnice, ale i jako pomůcka pro překlad mezi těmito dvěma jazyky a zapamatování slov v uvedeném slovníku. Poznámka 17: Hypotéza, že Mnišovský napsal knihu jako učebnici češtiny pro svého žáka Ferdinanda, zmíněná v literatuře, je zřejmě nesprávná. Ferdinand se stal žákem Mnišovského v roce 1619, ale kniha byla napsána roku 1628, v době, kdy byl Mnišovský už sekretářem císařské kanceláře. Její formát je takový, že by se z ní Ferdinand česky nenaučil a navíc už v roce 1627, rok před napsáním knihy, mluvil Ferdinand česky plynně. Také pokud by ji psal Mnišovský pro následníka trůnu, jistě by v úvodu uvedl věnování." Poznámka 18: Rukopis je už zmíněn v katalogu královny Kristýny z roku 1649, viz: C. Davidsson, c.p. s. 148. "* (konec citátů, j.h.)

Není třeba říkat, že citáty jsou z knihy vydané Karlovou univerzitou v Praze, tedy výsledkem seriózního vědeckého výzkumu. Z toho pak můžeme navíc udělat několik závěrů:

a) Kniha tedy nejen není učebnice češtiny, ale nebyla dokonce ani psána pro následníka trůnu (škoda, mohla by někde být i druhá kopie :-). Sám Mnišovský uvádí lingvistické použití knihy jakožto sekundární, ne jako hlavní účel.

b) Kniha nemá věnování, což je na tu dobu neobvyklé. Neměla snad být nikdy určena pro tisk? A kterému jinému účelu měla sloužit? Zde můžeme jenom hádat. Je zajímavé, že VM také nemá žádnou druhou kopii.

c) Pokud tedy Mnišovský VM napsal, musel ho napsat až po této své knize. Proč? Pouze po studii materiálu v této knize by poznal, jak je jeho šifra nedostačující a vymyslel by lepší šifru (a celý podvrh). Na to by ale potřeboval pergamen, jeho "Constructio" je psáno na papíře. A co je důležité, kódování ve VM je zřejmě daleko rafinovanější než šifra v jeho knize. Takže VM by se mohl objevit až po roce 1628, ale ještě před rokem 1637 (kdy už o VM píše Bareš ve svém dopise Kircherovi). Také datum z Wikipedie, tj. objevu nové šifry je zřejmě mylné. V roce 1618 ještě Mnišovský neměl ani jednoduchou verzi Ave Maria. Pokud by přece jen tehdy měl něco lepšího, proč by se deset let po tom vracel k něčemu daleko primitivnějšímu? Zřejmě se ve Wikipedii jedná o překlep - namísto 1628, někdo to opsal jako 1618. Ten rok byl navíc rokem pražské defenestrace a Mnišovského kancelář ve Vídni měla jiné starosti, než vymýšlet šifry. Horčický už tehdy byl ve vězení a ostatní katolíci se různě schovávali. Komu by se o té šifře teda chlubil? Navíc jsem také našel v jeho knize, že se "vytahoval", Říká totiž v předmluvě ještě toto:"Occultus occulti scribendi modus quem nemo mortalium queat

penetrareo" (Metoda tajného písma, které žádný smrtelník nemůže rozluštit).

d) Víme zatím o třech chybách v minulosti: první je od Dobrovského, který popsal knihu jako učebnici (asi neměl ve Švédsku moc času si ji prohlédnout - jako češtinář by to jinak poznal hned) a pak Dudík, který nesprávně usoudil, že zkrácený podpis (Rafaël Mnisch., napsáno na konci knihy) znamení někoho jiného, jakéhosi Mniše. Třetí chyba byla přisouzení knihy jako učebnice pro Ferdinanda III.

e) Mnišovského kniha pobývala v Čechách asi 20 let, odvezli ji do Švédska při drancování Prahy, 4 roky po jeho smrti. Protože se ale švédové nikdy nedostali přes Karlův most do Starého města (díky studentské mušketýrské milici, mezi kterou byl i profesor Marci; za což pak dostal šlechtický titul z Kronlandu), by patrně kniha uložena na pražském hradě. V té době (1648) už ale měl Bareš VM u sebe nejméně 11 let ...

Druhý objev

Objevil jsem kdesi poznámku, myslím, že to bylo v knize "Making of Habsburg Monarchy", od R.J.W. Evanse, že prý Mnišovský tvrdil, že studoval 30 let alchymii a sháněl pro Rudolfa II. rukopisy z různých klášterů. Jmenoval prý *Braunau* (to je v Rakousku, kde se později narodil Hitler, ne, vážně!) a *Kremsmunster* (v Horních Rakousích, kde je klášter a městečko samo bylo založeno v roce 777, je tedy dost staré, aby tam nějaký starý rukopis nalezen byl :-)). V této souvislosti je zajímavá poznámka v knize prof. Newbolda, že mu Voynich řekl, že našel VM v jednom zámku v Rakousku, ale to je jistě jen náhoda. Ovšem, proč by zrovna nemohl Mnišovský najít VM sám a to přímo v Rakousku?

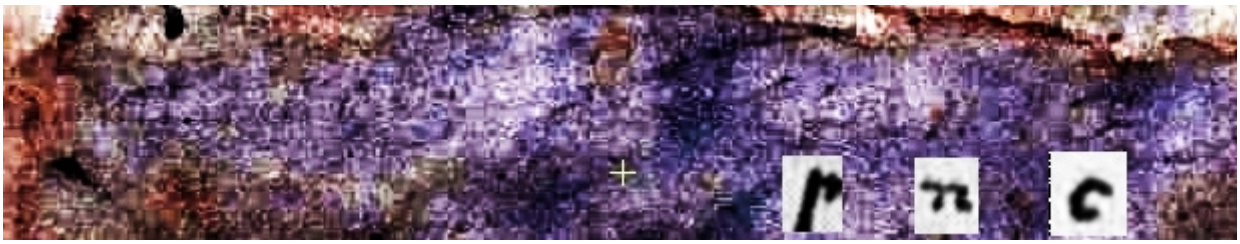
Ovšem mohlo to být naopak, třeba právě tam dostal nápad udělat podvrh. Proč by vlastně nemohl VM napsat on? Víme, že byl odborník na kryptologii své doby, takový, že dokonce mohl o tom psát knihy. To nám také zodpoví, kde by mohl někdo jako Mnišovský sehnat tolik listů pergamenu. Víme, že se také zajímal o alchymii. Ale co jeho písmo? Už z ukázky jeho knihy vidíme, že bylo netypické, nikdo jiný, kterého jsme zkoumali, neměl tolik oddělené písmo (prakticky každé písmeno bylo psané zvlášť, bez spojení s jeho sousedními písmeny). Ano, přesně tak, jako ve VM. Věty ve VM totiž nemají tečky ani čárky a odstavce, které bereme dnes jako věty, jsou v průměru 30 až 70 "slov". Jsou tedy trochu delší než třeba české či jiné věty, ale to se zatím žádnému výzkumníkovi nezdálo podezřelé :-).

Na druhé straně, pro Ave Maria by "věty" byly příliš krátké (jedno slovo=jedno písmeno), takže šifra z Mnišovského knihy asi nebyla použita ve VM. To ovšem neeliminuje Mnišovského coby autora, ale ani ne Trithemia, protože oba byli schopni přijít ještě s něčím jiným, než co napsali. Mnišovský navíc ještě vylepšil metodu Trithemia, což se málokomu v té době podařilo. Kromě Bacona a Johna Dee, Mnišovský je vlastně jediný znalec kryptografie, jmenovaný v Marciho dopise. A co víc: musel znát práce Trithemia velmi dobře, dokonce ho jmenuje v úvodu své knihy. Zřejmě se také od něj hodně naučil. A kdyby byl býval opravdu napsal náš VM, mohl by se opravdu chlubit tím, že vymyslel nerozluštitelnou šifru :-)

Třetí objev

Nedávno jsem objevil ještě něco: nápaditou podobnost Mnišovského rukopisu s rukou, která

napsala jméno Horčického do VM. Zde je ukázka slova Tepenec s proloženými písmeny z Mnišovského knihy:



Je to zřejmě nejblíže ze všech rukopisů autorů (rozuměj jejich rukou), co jsem studoval. To neznamená, že jsem zcela uspokojen tou podobností, ale asi už lepší "ruku" nenajdeme. To samo ovšem ještě neznamená, že napsal i celý VM, ale stačí to jako důkaz, že možná jednou měl VM ve vlastnictví. Koneckonců jsme už dokázali, že to nebyl Horčický, co se tam podepsal (viz můj článek "NOVÝ PODPIS HORČICKÉHO). Ovšem proč by tam Mnišovský napsal právě Horčického jméno a jak mohl vědět, že Horčický jednou knihu vlastnil, to se můžeme jen dohadovat. Přidejme k tomu, že Mnišovský se "zapomněl" o svém vlastnictví VM zmínit Marcimu, když ten se ho ptal a můžeme znovu zapochybovat o celé té historce. Ovšem to by zatřáslo základy staré, stále opakované historky o císaři sběrateli, anglickém mágovi a středověkém mnichu Baconovi ...

Odkazy

[1] Hurych, J. B.: THE MYSTERIOUS DR. RAPHAEL.
URL <http://hurontaria.baf.cz/CVM/a19.htm>.

[2] Hurych, J. B.: THE RESEARCH OF THE VOYNICH MANUSCRIPT: The Strategies and the Results. URL <http://hurontaria.baf.cz/CVM/a20.htm>.

[3] Hurych, J. B.: MORE ABOUT DR. RAPHAEL MNISHOWSKY.
URL <http://hurontaria.baf.cz/CVM/a22.htm> .

[4] Hurych, J. B.: ZÁHADNÝ DR. RAFAEL.
URL <http://hurontaria.baf.cz/VM/v2050.htm>.

[5] Hurych, J. B.: JEŠTĚ O DR. RAFAELOVI.
URL <http://hurontaria.baf.cz/VM/v2052.htm>.

E. O čem jsme psali v dubnu 2000 – 2007

Crypto-World 4/2000

Crypto-World 4/2001

Crypto-World 4/2002

Crypto-World 4/2003

Crypto-World 4/2004

Crypto-World 4/2005

Crypto-World 4/2006

Crypto-World 4/2007

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/